

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE



**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA ELEKTROTECHNIKY**

**A KOMUNIKAČNÍCH TECHNOLOGIÍ**

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

**ÚSTAV TELEKOMUNIKACÍ**

DEPARTMENT OF TELECOMMUNICATIONS

**AGREGACE LINEK NA SÍŤOVÝCH PRVCÍCH MIKROTIK**

LINK AGGREGATION USING MIKROTIK NETWORK NODES

**BAKALÁŘSKÁ PRÁCE**

BACHELOR'S THESIS

**AUTOR PRÁCE**

AUTHOR

**Roman Surový**

**VEDOUCÍ PRÁCE**

SUPERVISOR

**doc. Ing. Jaroslav Koton, Ph.D.**

**BRNO 2017**



# Bakalářská práce

bakalářský studijní obor **Teleinformatika**

Ústav telekomunikací

**Student:** Roman Surový

**ID:** 164946

**Ročník:** 3

**Akademický rok:** 2016/17

**NÁZEV TÉMATU:**

## Agregace linek na síťových prvcích Mikrotik

### POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s principy a možnostmi agregace síťových linek. Získané poznatky uplatněte při konfiguraci a testování výkonnosti síťových prvků Mikrotik provozovaných v režimech např. dle IEEE802.3ad, balance-rr a dalších. Vlastnosti vybraných režimů znázorníte na příkladech, kdy bude demonstrován jak bezchybný provoz, tak provoz při výpadku a opětovném zprovoznění některé z linek. Za základě získaných výsledků diskutujte scénáře a místa nasazení jednotlivých mechanismů.

### DOPORUČENÁ LITERATURA:

[1] TANENBAUM, A.S., WETHERALL, D.J.: Computer networks, Pearson, 2010, ISBN: 978-0132126953.

[2] Manual: Interface/Bonding. Mikrotik documentation [online]. 2016 [cit. 2016-09-12]. Dostupné z: <http://wiki.mikrotik.com/wiki/Manual:Interface/Bonding>

**Termín zadání:** 1.2.2017

**Termín odevzdání:** 8.6.2017

**Vedoucí práce:** doc. Ing. Jaroslav Koton, Ph.D.

**Konzultant:**

**doc. Ing. Jiří Mišurec, CSc.**  
*předseda oborové rady*

### UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## **ABSTRAKT**

Cielom tejto bakalárskej práce je zoznámiť sa s princípmi a možnosťmi agregácie sieťových liniek. Získané poznatky následne uplatniť pri konfigurácii a testovaní výkonnosti sieťových prvkov MikroTik prevádzkovaných v režimoch napríklad podľa IEEE802.3ad, balance-rr a mnoho ďalších. Vlastnosti vybraných režimov budú znázornené, kde bude demonštrovaná bezchybná prevádzka, ako aj prevádzka pri výpadku a pri opätovnom zprovoznení niektorých liniek.

## **KLÍČOVÁ SLOVA**

IEEE802.3ad, ARP Pozorovanie, MII Pozorovanie, Rovnováha-rr, Aktívna záloha, Rovnováha-xor, Broadcast, Rovnováha-tlb, Rovnováha-alb

## **ABSTRACT**

The aim of this Bachelor thesis is to get acquainted with the principles and option of aggregation network lines. Then apply the acquired knowledge in configuring and testing the performance of network elements in MikroTik operating modes, for example, by IEEE802.3ad, balance-rr, and many others. Properties of the selected mode will be shown, which will be demonstrated error-free operation. As well as operation and case of failure in re-configuring for some lines.

## **KEYWORDS**

IEEE802.3ad, ARP Monitoring, MII Monitoring, Balance-rr, Active-Backup, Balance-xor, Broadcast, Balance-tlb, Balance-alb

SUROVÝ, Roman *Agregace linek na síťových prvcích Mikrotik*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2017. 42 s. Vedoucí práce byl doc. Ing. Jaroslav Koton, Ph.D.

## PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Agregace linek na síťových prvcích Mikrotik“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno .....

.....

podpis autora(-ky)

## PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Jaroslavi Kotonovi Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno .....

.....

podpis autora(-ky)

# OBSAH

Úvod	8
<b>1 Agregácia liniek v sieti</b>	<b>9</b>
1.1 Agregácia liniek . . . . .	9
1.2 IEEE Agregácia zväzkov . . . . .	10
1.2.1 Proces štandardizácie . . . . .	10
1.2.2 Počiatočný protokol 802.3ad . . . . .	11
1.2.3 LACP a LAG . . . . .	11
1.2.4 Výhody oproti statickej konfigurácii . . . . .	13
<b>2 MikroTik</b>	<b>14</b>
2.1 História MikroTiku . . . . .	14
2.2 RouterOS . . . . .	14
2.3 Winbox . . . . .	15
2.4 Bonding . . . . .	16
2.4.1 Sprievodca nastavením smerovačov . . . . .	17
2.4.2 Pozorovanie spojenia . . . . .	18
2.5 Mody Bondigu . . . . .	18
2.5.1 802.3ad . . . . .	18
2.5.2 Balance-rr . . . . .	21
2.5.3 Active backup . . . . .	21
2.5.4 Balance-xor . . . . .	22
2.5.5 Broadcast . . . . .	22
2.5.6 Balance-tlb . . . . .	22
2.5.7 Príklad konfigurácie Balance-tlb . . . . .	22
2.5.8 Balance-alb . . . . .	23
2.6 Address Resolution Protocol Monitoring . . . . .	23
2.7 Media independent interface Monitoring . . . . .	25
2.8 Transmit hash policy . . . . .	26
<b>3 Výsledky merania v laboratóriu</b>	<b>27</b>
3.1 Zapojenie . . . . .	27
3.2 Meranie 802.3ad . . . . .	27
3.3 Meranie Balance-rr . . . . .	29
3.4 Meranie Active-backup . . . . .	31
3.5 Meranie Balance-tlb . . . . .	31
3.6 Meranie Balance-alb . . . . .	32

3.7	Meranie Broadcast . . . . .	32
3.8	Meranie Balance-xor . . . . .	32
3.9	Porovnanie všetkých režimov . . . . .	33
<b>4</b>	<b>Závěr</b>	<b>39</b>
	<b>Literatura</b>	<b>40</b>
	<b>Seznam symbolů, veličin a zkratk</b>	<b>42</b>



# ÚVOD

V tejto bakalárskej práci sa budem zameriavať na agregáciu liniek na sieťových prvkoch MikroTik postupne vysvetlím a poukážem na základné vlastnosti agregácie liniek z čoho agregácia pozostáva aké protokoly ju zahrnujú, ktoré typy môžu existovať. Poukážem na jej základné a dôležité časti ako aj na aké hlavné časti sa rozdeľuje, aké sú jej hlavné vlastnosti a históriu. Prečo je dôležitou súčasťou nášho života a na čo ju môžeme použiť.

Ak chceme komunikovať alebo prenášať veľké objemy dát, ktorých je každodenne na internete viac a viac, mali by sme rozumieť tomu akými spôsobmi sa v internetových a počítačových sieťach pracuje. Čo sa týka komunikačných protokolov, sú neoddeliteľnou súčasťou virtuálneho sveta. Bez komunikačných protokolov by sme neboli schopní prenášať súbory a rôzne dáta.

V prvej kapitole tejto bakalárskej práce sa zaoberáme agregáciou liniek jej základnými štandardami vysvetlíme z čoho pozostáva, popíšeme si ju. Poukážeme na jej históriu dôležité osoby ktoré sa k nej priblížili. V praxi totižto možno agregáciu využiť na všetkých troch vrstvách OSI modelu.

V druhej kapitole sa venujeme samotnému MikroTiku. Popíšeme si vznik tejto spoločnosti kde sa nachádza čím sa zaoberá popisujeme jej využitie, akými hlavnými systémami sa zaoberá. Popíšeme si jej hlavný produkt ďalej softvér, ktorý už vyrába niekoľko úspešných rokov a veríme, že bude pokračovať aj naďalej pretože vykazuje veľmi dobré výsledky. Popíšeme si ako sa pripojiť k samotnému MikroTiku, ktorý program sa dá nato využiť. Ďalej si podrobne vysvetlíme samotný bonding, ktorý je samozrejme dôležitou súčasťou tejto práce.

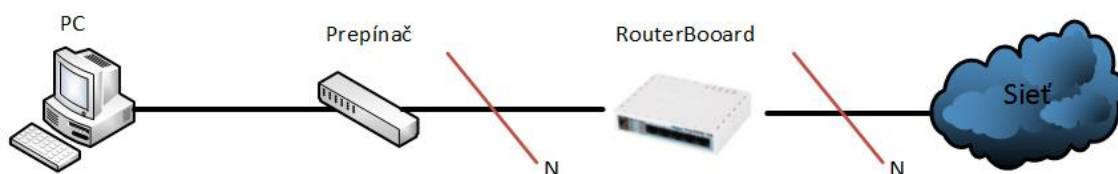
V tretej kapitole sa venujeme získaným poznatkom a následne ich uplatňujeme pri konfigurácii a testovaní výkonnosti sieťových prvkov MikroTiku v prevádzkovaných režimoch napríklad podľa IEEE802.3ad, balance-rr a mnoho ďalších, tu sledujeme sieťový prenos medzi MikroTikom, prepínačom a počítačom. Práca zahrnuje aj využitie v praxi a omedzenia agregácie sieťových liniek ako aj podrobnejší opis jednotlivých metód a využití.

# 1 AGREGÁCIA LINIEK V SIETI

V prvej kapitole sa budeme zaoberať agregáciou liniek v sieti, povieme si jej históriu zadefinujeme si ju uvedieme jednotlivé príklady pri vrstvách. Zadefinujeme jednotlivé protokoly ako 802.3ad, 802.1 layer. Vysvetlíme si agregáciu zväzkov, linkovú agregáciu kontrolovanú protokolom.

## 1.1 Agregácia liniek

Samotná agregácia liniek je termín kde sa jedná o vzťahy na rôzne spôsoby kombinovania agregácie to znamená viac sieťových pripojení ktoré sú paralelne prepojené či už počítač s počítačom alebo prepínač s počítačom a to nad rámec priepustnosti toho čo dokáže jedno spojenie udržať a zabezpečiť tak redundanciu to aj v prípade, že by jedna z liniek vypadla. Na obr. 1.1 možno vidieť pripojenie kde môže byť využité veľké množstvo pokračujúcich pripojení a tým aj samotná agregácia liniek dokumentáciu Agregácie nájdete na: [15]



Obr. 1.1: Príklad pripojenia

Oneskorenie „Link Aggregation Group“ v sebe môže spájať celý rad fyzických portov dohromady, spôsobuje to jediná cesta dát s vysokou priepustnosťou pre opravu môžeme naplňať zdieľanie dopravnej záťaže medzi členské porty v skupine a to nám zabezpečí zvýšenie spoľahlivosti spojenia.

Siete môžu byť implementované architektmi agregáciou na niektoré z najnižších troch vrstiev OSI modelu.

### Príklady s agregáciou:

- U prvej vrstvy OSI modelu, čiže fyzická vrstva sú zahrnuté elektrické vedenia je to napríklad IEEE 1901, alebo bezdrôtové IEEE 802.11 či už sieťové zariadenia, ktoré nám kombinujú viac frekvenčných pásiem.
- U druhej vrstvy OSI modelu, kde sa jedná o dátovú vrstvu, to môže byť napríklad Ethernet v sieťach LAN, alebo multi-link PPP WAN, Ethernet MAC

adries. Ku agregácii zvyčajne dochádza naprieč niektorými z portov prepínača, ktoré môžu byť buď fyzické porty alebo virtuálne no tie sú riadené operačným systémom.

- Agregácia na tretej vrstve, sieťová vrstva v OSI modeli tu možno použiť v „round-robin scheduling“ čo znamená, že procesor sa rozhodne aký proces mu bude pridelený a ďalším sú hash hodnoty ktoré sú vypočítané z polí v hlavičke paketu alebo kombináciou týchto dvoch metód.

Bez ohľadu na to, na ktorej vrstve môže vzniknúť agregácia, sieťový výkon je vyrovnaný na všetkých zväzkoch. Väčšina metód nám poskytuje taktiež failover.

Kombinácia sa môže objaviť aj tak, že hromadné rozhrania spájajú jednu logickú adresu (napr IP) alebo jednu fyzickú adresu (napr MAC) alebo môže mať každé rozhranie vlastnú adresu. Síce si to vyžaduje, aby oba konce zväzku používali rovnakú agregáčnú metódu, ale má to výhodu aj vo výkone.

Agregácia zväzkov čelí dvom problémom s ethernet spojením a to limit šírky priepustnosti a nedostatok pružnosti.

Vzhľadom na prvý problém požiadavky šírky priepustnosti sa nemenia lineárne. Z historického pohľadu sa Ethernet rozhrania zvýšilo desaťnásobne každou generáciou o 10 Megabit/s, 100 Mbit/s, 1000 Mbit/s, 10,000 Mbit/s, keď sa však už blížil strop šírky rozhrania, jediná možnosť bola posunúť sa k ďalšej generácii, ale to by bolo skoro nemožné kvôli nákladom pretože tie sú vždy dôležité. Alternatívne riešenie, ktoré predstavilo veľa výrobcov v skorších 1990, kombinuje dve fyzické ethernet spojenia do jedného logického zväzku cez káblové spájanie. Veľa z týchto riešení vyžadovalo manuálnu konfiguráciu a rovnaké vybavenie na oboch stranách agregácie.

Druhý problém zahŕňa tri jednotlivé body zlyhania v typickom spojení port s káblom a portom. Buď v bežnej konfigurácii počítač s prepínačom alebo v prepínači s prepínačom tento kábel ako taký, alebo niektorý z portov do ktorého je kábel zapojený, nám môžu zlyhať. Môžeme vytvoriť tak viacnásobné fyzické prepojenia, ale veľa z protokolov vyššej úrovne neboli vytvorené k úplne bezproblémovému failoveru. Failover je vysvetlený v kapitole Bondingu.

## 1.2 IEEE Agregácia zväzkov

### 1.2.1 Proces štandardizácie

V procese štandardizácie do polovice 1990, väčšina výrobcov sieťových prepínačov obsahovala kapacitu agregácie ako vlastnú patentovú nadstavbu, aby tým zvýšili šírku rozhrania medzi prepínačmi, ale každý výrobca vyvinul vlastnú metódu, čo

viedlo k veľa problémom s kompatibilitou. Preto IEEE 802.3 group založila v novembri 1997 skupinu, ktorá sa zaoberala vytvorením štandardu, ktorý by bolo možné použiť všeobecne. Toto prišlo známe ako "Link Aggregation Control Protocol" v preklade "Linková Agregácia kontrolovaná protokolom."

### 1.2.2 Počiatočný protokol 802.3ad

V roku 2000 väčšina gigabitových spájaných kanálov používala štandard IEEE agregácie liniek odkaz na dokumentáciu 802.3ad protokolu: [14] ktorý bol predtým klasifikovaný ako 43 štandard IEEE 802.3, ale ako pridaná hodnota a to v Marci roku 2000 už bol ako 802.3ad. Takmer každý výrobca sieťových zariadení rýchlo prijal túto spoločnú normu ako ich vlastný štandard.

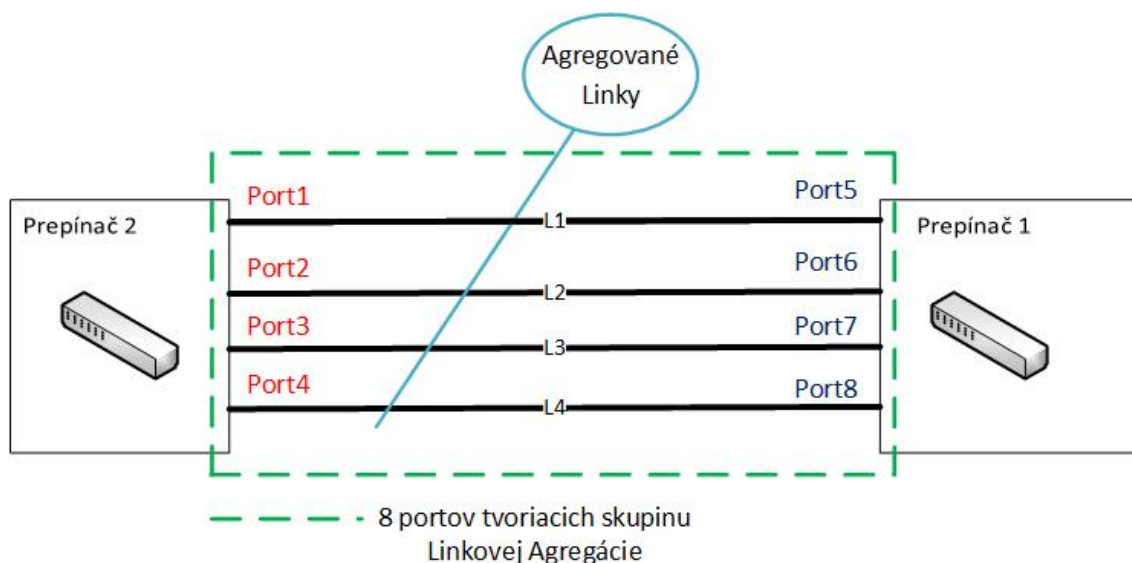
Presun na 802.1 vrstvy sa udial v roku 2008 a to za pomoci Davida Lawa ktorý sa stal známim v roku 2006 pre niektoré 802.1 vrstvy (ako je bezpečnosť 802.1X) ktoré boli umiestnené v zásobníku protokole pod linkovou agregáciou, ktorá bola definovaná ako 802.3 vyššia podvrstva siete. Tento rozpor bol však vyriešený s formálnym prevodom protokolu do skupiny 802.1 so zverejnením IEEE 802.1AX a to v roku 2008 dňa 3. novembra 2008.

### 1.2.3 LACP a LAG

Link Aggregation Groups (LAG) a Link Aggregation Control Protocol (LACP) odkaz na dokumentáciu LACP A LAG: [5] voľne preložené Linková Agregácia v skupine a Linková Agregácia kontrolovaná protokolom sú metódy na poskytovanie viac ako jednej väzby medzi dvoma prepínačmi a automatizovať tieto konfigurácie a údržby, respektíve pozrime sa na dôvod, prečo sú LAG a LACP potrebné ich výhody zapojení linky. Na obr. 1.2 môžeme vidieť kombináciu viacerých liniek medzi dvoma zariadeniami vedenú z jednej veľkej linky.

LAG pre pripojenie cez dva prepínače, používame kábel pre prepojenie dvoch fyzických portov jeden v každom prepínači a treba ho nakonfigurovať ako kmeňový. Ale jeden kmeňový musí mať obmedzenú šírku pásma. Môžeme použiť stohovanie a získať tak väčšiu šírku pásma, ale stohovanie je väčšinou proprietárne a podporuje iba obmedzenú vzdialenosť. Za účelom získania širokopásmových štátnych liniek medzi dvoma prepínačmi, alebo dve zariadenia môžeme použiť LAG.

V IEEE špecifikácie sa Linková Agregácia kontrolovaná protokolom poskytuje ako spôsob pre riadenie zoskupenia viacerých fyzických portov ktoré môžu spolu tvoriť jediný logický kanál. Linková Agregácia kontrolovaná protokolom umožňuje,



Obr. 1.2: Kombinácia viacerých liniek

že sieťové zariadenie môže vyjednať automatické zväzovanie odkazov zaslaním Linkovej Agregácie kontrolovanej protokolom paketov do peer (priamo pripojeného zariadenia, ktoré tiež implementuje LACP).

Funkcia Linkovej Agregácie kontrolovanej protokolom a jej praktické príklady:

1. Maximálny počet združených portov povolených v kanálovom porte: Platné hodnoty sú obvykle od 1 do 8.
2. LACP pakety sú odosielané so skupinou multicast MAC a to s adresou 01:80:C2:00:00:02 (01-80-c2-00-00-02)
3. Počas trvania LACP pakety sú prenášané každú sekundu a snažia sa udržať nažive mechanizmus pre väzobného člena štandardne je to pre pomalé = 30s a rýchle = 1s.
4. LACP môže mať kanálový port v režime vyváženého linka alebo linka-id čiže celé číslo, ktoré určí prepojenie členov pre vyrovnanie zaťaženia. Rozsah je od 1 do 8.
5. LACP v aktívnom režime umožňuje LACP bezpodmienečne. V nečinnosti umožňuje LACP iba vtedy, keď je detegovať LACP alebo zariadenie. Tomuto sa hovorí východiskový stav.

### 1.2.4 Výhody oproti statickej konfigurácii

1. Failover prebieha automaticky ak odkaz zlyhá a ak tam je napríklad mediálny prevodník medzi zariadeniami, bude peer systém ignorovať problémy alebo nebude brať ohľad nad pripojením. So statickou linkovou agregáciou peer bude aj naďalej posielat prevádzku preruší len ak spojenie spôsobuje zlyhanie pripojenia.
2. Dynamická konfigurácia prístroja sa môže potvrdiť tak že konfigurácia na druhom konci môže spracovávať linkovú agregáciu. So statickou linkovou agregáciou a to s kabelážou, alebo s konfiguračnou chybou môže zostať nepovšimnutá a tým spôsobiť nežiaduce účinky na sieti.

## 2 MIKROTIK

V druhej časti práce sa budeme zameriavať na samotný MikroTik. Vysvetlíme si čo táto spoločnosť vyrába a dosiahla, aké sú jej hlavné ciele, akými hlavným systémom sa zaoberá. V ďalšej časti si podrobne vysvetlíme samotný bonding ktorý je pre túto bakalársku prácu dôležitý. Opíšeme si aké zapojenia môžu pri agregácii liniek nastať a ako ich aplikovať.

### 2.1 História MikroTiku

Spoločnosť MikroTiks, tikls čo v preklade znamená sieť je vo svete skôr známa ako MikroTik odkaz na dokumentáciu MikroTiku: [7] a bola založená v roku 1996 zaoberá sa hlavne vývojom a predajom bezdrôtových systémov k rozvoju smerovača. Z tých najznámejších je to ISP.

V súčasnosti poskytuje hardvér a softvér pre bezdrôtové systémy a internetovú konektivitu pre veľa miest na svete a to snáď v každej krajine. Má bohaté skúsenosti s používaním PC hardvéru ako aj softvéru a kompletných systémov pre smerovanie umožnil to totiž softvér vyvinutý v roku 1997. Tento softvér je známy pod menom RouterOS, ktorý poskytuje rozsiahlu stabilitu pre ovládanie, flexibilitu všetkých druhov dátových rozhraní a to aj smerovanie. V roku 2002 sa spoločnosť rozhodla vytvoriť vlastný hardvér jeho značka bola pomenovaná RouterBOARD.

Spoločnosť MikroTiks sa nachádza v Lotyšsku v meste Riga čo je hlavné mesto Lotyšska a má viac ako 140 zamestnancov.

### 2.2 RouterOS

Hlavným produktom spoločnosti MikroTik je operačný systém založený na linuxovom jadre známy ako MikroTik RouterOS odkaz na dokumentáciu RouteruOS: [11]. RouterBOARD 493C, ktorý budeme používať v našej bakalárskej práci môžete vidieť na obr. 2.1. Tento operačný systém bol inštalovaný na hardvér zo série RouterBOARD, alebo na štandardných počítačoch s procesorom x86. Z toho vyplýva, že počítač cez smerovač môže realizovať rôzne ďalšie funkcie ako napríklad firewall čo je vlastne určitá kontrola údajov, ktorá prebieha na základe aplikovania, alebo porovnávania niektorých pravidiel, ktoré nám určujú podmienky prípadne niektoré akcie. Ďalšou časťou realizácie je virtuálna privátna sieť VPN prostredníctvom ktorej sa užívateľ môže pripojiť na rôznych miestach pomocou internetu ďalej bandwidth shaping ktorý zabezpečuje proces pridelenia častí sieťových pripojení, ktorým sa stanovuje množstvo šírky pásma.



Obr. 2.1: RouterBOARD 493C

Systém sa tiež dokáže chovať ako captive portal umožňuje to pripojiť sa na inú stránku ktorá sa objaví ako prvá pri pripojení do cudzej siete. Taktiež systém sa môže chovať ako hotspot ide o zdieľanie siete.

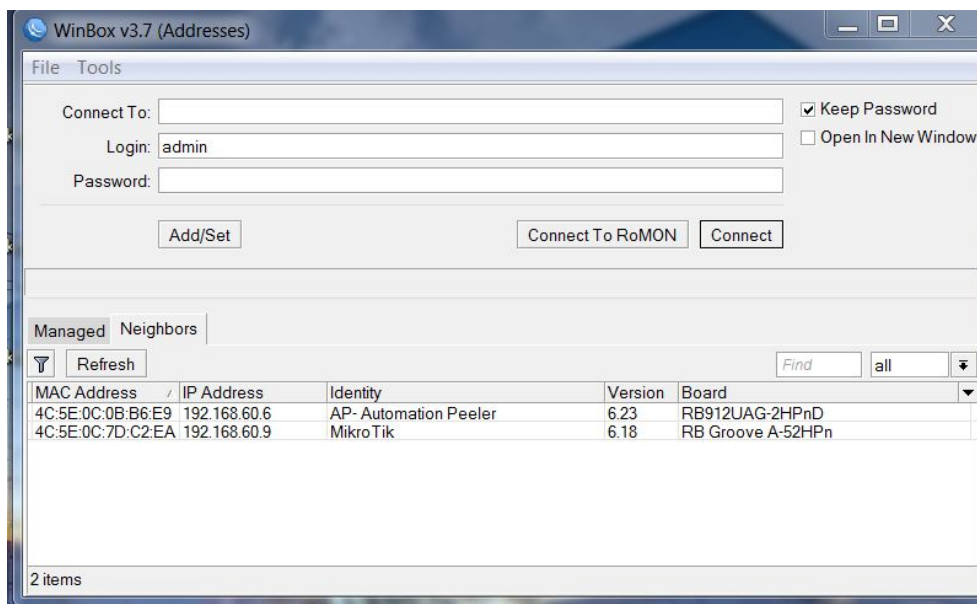
Operačný systém je licencovaný tým si spoločnosť zabezpečuje zvyšovanie a skvalitnenie úrovne služieb každá úroveň uvoľní viac dostupných funkcií pre RouterOS. Aplikácia MS Windows s názvom Winbox poskytuje kvalitné grafické, užívateľské rozhranie pre konfiguráciu a monitorovanie operačného systému RouterOS. RouterOS tiež umožňuje prístup cez FTP, telnet a SSH (Secure Shell).

## 2.3 Winbox

Winbox nástroj, ktorý umožňuje administrátorovi pripojiť sa k MikroTiku RouterOS odkaz na dokumentáciu Winboxu: [6] pomocou rýchleho a jednoduchého GUI. Jedná sa o domorodý program Win32 ktorý je riadený binárne, ale môže bežať aj na Linuxe a MacOS (OSX) pomocou Wine. Všetky funkcie vo Winboxe sú riadené konzolou, to je dôvod, prečo tam nie sú žiadne Winbox manuály v príručke. Niektoré z moderných systémov kritických konfigurácií nie sú možné vo Winboxe, rovnako ako zmeny MAC adresy na rozhraní.

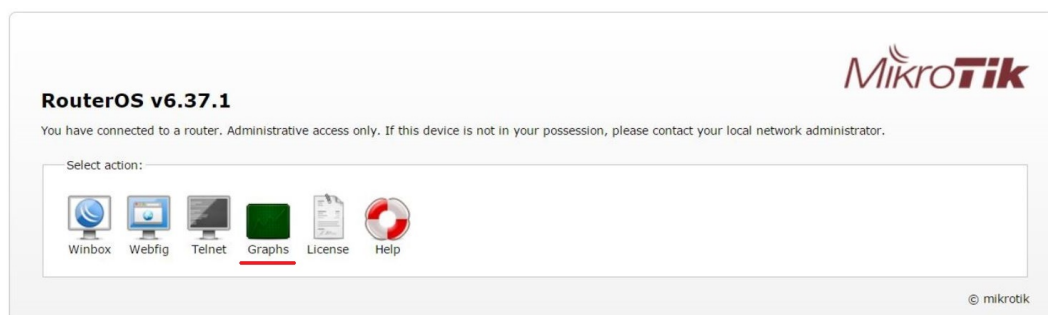
Ak sa chceme pripojiť k MikroTiku stačí zadať IP alebo MAC adresu smerovača, ako vidno na obr. 2.2 treba zadať meno a heslo samozrejme ak existuje a kliknúť na tlačidlo Connect pre pripojenie. Môže sa tiež zadať číslo portu IP adresy, avšak treba ho oddeliť dvojbodkou, ako je napríklad tento 192.168.88.1:9999. Port sa dá





Obr. 2.2: Pripojenie do Winboxu

zmeniť v ponuke RouterOS služieb. No druhý spôsob je možný pomocou akéhokoľvek webového prehliadača kde je, ale treba najprv spraviť prvotné povolenie, v samotnom winboxe, sú v ňom možno vidieť grafické znázornenia vyťaženia jednotlivých častí hardvéru a veľa ďalších užitočných vlastností ktoré vidno na obr. 2.3 tá najdôležitejšia je vyznačená červeným, lebo tu práve v tejto práci použijeme.



Obr. 2.3: Pripojenie pomocou webového prehliadača

## 2.4 Bonding

Bonding čiže voľne preložené spájanie odkaz na dokumentáciu bonding: [1] je technológia, ktorá nám umožňuje agregáciu viacnásobných ethernetových rozhraní do

jednotného virtuálneho zväzku, zvyšuje sa tak rýchlosť dát a poskytuje nám aj spomínaný failover.

Detekcia zlyhania linky a failover funguje podstatne lepšie s drahšími sieťovými kartami, než s lacnejšími dobrým príkladom je Intel. Pri Intel kartách totiž trvá menej než sekundu failover po stratení spojenia, pokým na iných kartách nám to zaberie až do 20 sekúnd čo je určite nepríjemne z hľadiska funkčnosti. Taktiež nám vyrovňovanie aktívneho nákladu na niektorých lacných kartách nefunguje.

Failover odkaz na dokumentáciu failoveru: [8] je prechod počítača do pohotovostného režimu, alebo pri výpadku je to abnormálne ukončenie predtým aktívnych aplikácií, servera, systému, hardvérových súčasti, alebo samozrejme v sieti. Failover je vlastne prevzatie služieb pri zlyhaní je to celkom automatické a zvyčajne pracuje bez varovania.

### 2.4.1 Sprievodca nastavením smerovačov

Predpokladajme, že máme 2 NICs v každom smerovači (R1 a R2) a chceme získať maximálny obnos dát medzi dvoma smerovačmi. Pre umožnenie môžeme nasledovať napríklad takto. Uistíme sa, že rozhrania nemajú IP adresy, ktoré by mohli byť podriadené pri spájaní rozhrania!

Pridáme spájajúce rozhranie na R1:

```
[admin@R1] interface bonding> add slaves=ether1,ether2
```

Pridáme R2:

```
[admin@R2] interface bonding> add slaves=ether1,ether2
```

Pridáme adresy k spájacím sa rozhraniám:

```
[admin@R1] ip address> add address=172.16.0.1/24 interface=bonding1  
[admin@R2] ip address> add address=172.16.0.2/24 interface=bonding1
```

Otestujeme link z R1:

```
[admin@R1] interface bonding> /pi 172.16.0.2  
172.16.0.2 ping timeout  
172.16.0.2 ping timeout  
172.16.0.2 ping timeout  
172.16.0.2 64 byte ping: ttl=64 time=2 ms  
172.16.0.2 64 byte ping: ttl=64 time=2 ms
```

Toto spájacie rozhranie potrebuje zopár sekúnd, aby sa spojilo so svojim peerom.

## 2.4.2 Pozorovanie spojenia

Je to pre nás rozhodujúce, či je aktivovaná niektorá z možných pozorovacích možností. V príklade hore, ak by niektorá zo spojenej linky mala zlyhať, spájajúci ovládač by stále pokračoval v posielaní paketov cez odpojenú linku, čo by viedlo k úpadku siete.

Spájanie v RouterOS súčasne podporuje dva spôsoby, ako pozorovať tento stav spojenia podriadených prístrojov: MII a ARP pozorovanie ktoré je vysvetlené nižšie v tejto kapitole nie je, ale možné použiť obe metódy naraz kvôli obmedzeniam v spájajúcom sa ovládači.

## 2.5 Mody Bondigu

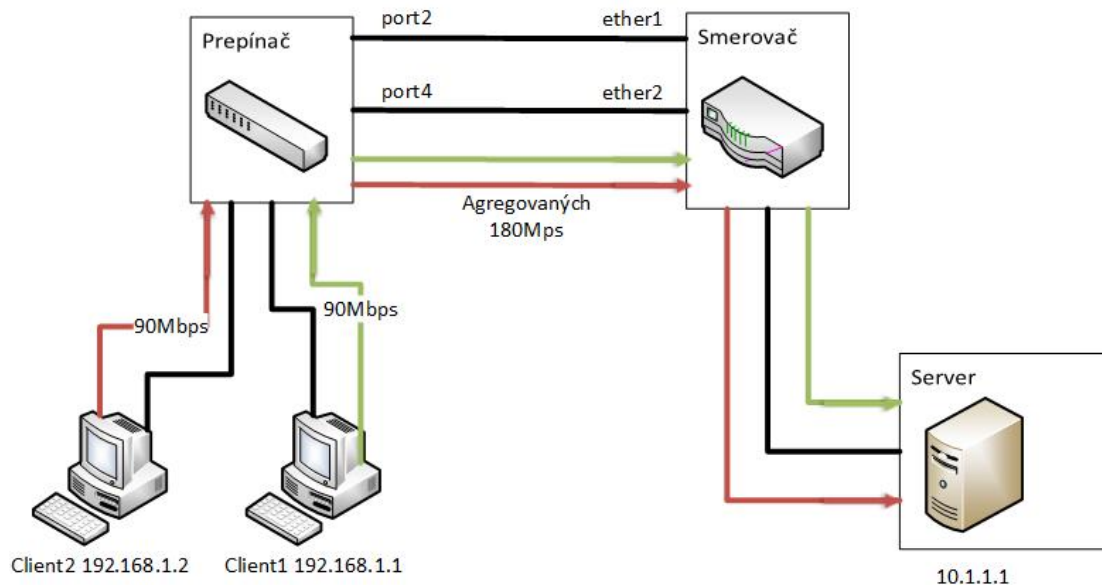
Tu sú spomenuté jednotlivé režimy ktoré môžeme použiť pri konfigurácii, podľa vhodného výberu a konfigurácii spojenia.

### 2.5.1 802.3ad

802.3ad režim je v IEEE štandarde tak isto volaný LACP „Link Aggregation Control Protocol/Agregácia liniek kontrolovaná protokolom“. LACP je vysvetlený pri Agregácii vyššie. Zahŕňa automatickú konfiguráciu celkov, takže je potrebné minimálne nastavovanie prepínača. Tento štandard tak isto nariaďuje, že rámec bude doručený v poradí a žiadne nesprávne usporiadania paketov sa v spojení nevyskytnú. Štandard nariaďuje aj to, že všetky prístroje v celku pracujú rovnakou rýchlosťou a to v duplex režime, pracuje iba s MII pozorovaním linky.

Agregácia liniek kontrolovaná protokolom vyrovnáva všetky vychádzajúce prenosy v aktívnych portoch založených na hlavných informáciach s kontrolným súčtom hash a prijíma všetky vstupné prenosy z akéhokoľvek aktívneho portu. Kontrolný súčet zahŕňa aj ethernet zdroj aj cieľové adresy ak sú dostupné, tak VLAN ako zdrojová a cieľová adresa vo verzii IPv4/IPv6. Výpočet závisí na parametri transmit-hash-policy. Ním sa vyberá, ktorá transmit hash policy sa použije na slave výber v balance-xor a 802.3ad režime, dokumentácia bola použitá z [2]

Príklad ktorý spája dve ethernetové rozhrania môžeme vidieť na obr. 2.4 kde na smerovači do prepínaču ako jednotného, načítava vyvážené a bezporuchové linky. Môžeme pridať viac rozhraní, aby sa zvýšila priechodnosť a bezporuchovosť. Keď je nariadené usporiadanie rámcov na Ethernet linke, potom akýkoľvek prenos medzi dvomi prístrojmi vždy prebieha po rovnakej fyzickej linke, ktorá limituje maximálnu rýchlosť toho rozhrania. Prenosový algoritmus sa pokúša použiť čo najviac informácií aby rozlíšil rôzne toky prenosov a rovnováhu po prístupných rozhraniach.



Obr. 2.4: Príklad konfigurácie

Konfigurácia Smerovača R1:

```
/interface bonding add slaves=ether1,ether2 mode=802.3ad lacp-rate=30secs link-
monitoring=mii-1 transmit-hash-policy=layer-2-and-3
```

Konfigurácia na prepínači:

Intelligent Switch: Trunk Configuration

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	M1	M2
1	-	v	-	v	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Tu si môžeme všimnúť, že agregácia liniek kontrolovaná protokolom je aktivovaná na prvom smernicovom zväzku TRK1 a porty prepínača na prvom smernicovom sú spojené s „v“ flag. V našom prípade porty 2 a 4 sa spustia v agregácii liniek kontrolovanej protokolom. Môžeme si overiť, či agregácia liniek kontrolovaná protokolom naozaj funguje. Na prepínači by sme mali najprv overiť, či je aktivovaná agregácia liniek kontrolovaná protokolom a či naozaj beží:

```
Intelligent Switch : LACP Port State Active
Port State Activity   Port State Activity
2 Active
4 Active
```

Ďalej sa môžeme uistiť, že agregácia liniek kontrolovaná protokolom pracuje s naším smerovačom. Ak nám vypíše, že nevidíme oba porty, potom je niekde chyba a LACP nefunguje.

```
Intelligent Switch : LACP Group Status
GroupActor>Actor
[Partner]
Priority: 1 65535
MAC : 000E2E2206A9 000C42409426
PortNoKeyPriorityActivePortNoKey
Priority
2 513 1 selected 1 9 255
4 513 1 selected 2 9 255
```

Keď sme overili, že prepínač úspešne pracuje s naším smerovačom s LACP, môžeme spustiť prenos z C1 a C2 do servera a kontrolovať, ako prenos napreduje cez oboch spojených „podriadených“:

```
[admin@test-host] /interface> monitor-traffic ether1,ether2,bonding1
rx-packets-per-second: 8158 8120 16278
rx-drops-per-second: 0 0 0
rx-errors-per-second: 0 0 0
rx-bits-per-second: 98.8Mbps 98.2Mbps 197.0Mbps
tx-packets-per-second: 4833 4560 9394
tx-drops-per-second: 0 0 0
tx-errors-per-second: 0 0 0
tx-bits-per-second: 2.7Mbps 3.0Mbps 5.8Mbps
```

Na niektorých prepínačoch musíme nastaviť správny protokol spájania linky, aby sme umožnili rovnovážnu činnosť v oboch smeroch.

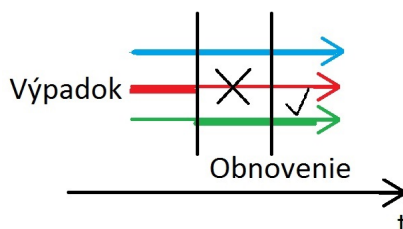
### 2.5.2 Balance-rr

Ak balance-rr voľne preložené rovnováha-rr, keď máme nastavený režim, pakety sú prenášané v sekvenčnom poradí od prvého dostupného slave do posledného. Rovnováha-rr je jediný režim, ktorý bude rozposielať pakety po viacnásobných rozhraniach, ktoré patria tomu istému TCP/IP spojeniu. Keď používame viacnásobné rozposielanie a prijímanie linky, pakety sú často prijímané mimo poradia, ktorého výsledkom bude opakované prijímanie segmentov, pre iné protokoly, ako UDP to ale nie je problém ak vie klientský softvér tolerovať pakety mimo poradia. Odkaz na dokumentáciu balance-rr: [1]

Ak už je použitý prepínač na hromadenie linky, potom je potrebné vhodné nakonfigurovanie portu prepínača, avšak veľa prepínačov nepodporuje rovnováhu-rr. Rýchly sprievodca nastavením predvädza použitie spájacieho režimu rovnováhy-rr. Ako môžeme vidieť, je to celkom jednoduché nastaviť. Rovnováha-rr je tak isto užitočná pri spájaní niekoľkých bezdrôtových liniek, avšak to si vyžaduje rovnakú šírku frekvenčného pásma pre všetky spájané linky. Ak sa zníži niektorá zo šíriek frekvenčného pásma, potom celková šírka spojenia sa bude rovnať najpomalejšej spájanej linke.

### 2.5.3 Active backup

Ďalej tu máme aktívnu zálohu po anglicky active backup. Tento režim využíva iba jedného aktívneho podriadeného na prenos paketov. Prídavný podriadený sa stáva aktívnym iba v prípade, že pôvodný podriadený zlyhá. To znamená že ak jedna z liniek vypadne druhá ju nahradí môžeme vidieť aj na obr. 2.5



Obr. 2.5: Aktívna záloha

MAC adresa spájaného rozhrania je zobrazená na aktívnom porte, aby sa predišlo zmäteniu prepínača. Aktívna záloha je najlepšia voľba pri nastaveniach s vysokým

využitím s viacnásobnými prepínačmi, ktoré sú prepojené avšak ARP pozorovanie v tomto prípade nebude správne fungovať, ak sú oba smerovače priamo prepojené. V nastaveniach mii-1 alebo mii-2 musí byť použité pozorovanie alebo medzi smerovačmi vložíme prepínač.

### 2.5.4 Balance-xor

Balance-xor tento režim vyvažuje výstupné prenosy cez aktívne porty založené na hlavnom protokole s kontrolným súčtom informácií a prijíma prichádzajúce prenosy zo všetkých aktívnych portov. Režim je veľmi podobný s LACP okrem toho, že nie je normovaný a pracuje s vrstvou 3 a 4 hash politikou.

### 2.5.5 Broadcast

Ak sú porty nakonfigurované s vysielacím režimom, všetky podriadené porty prenášajú rovnaké pakety do cieľových staníc aby sa zaistila bezchybnosť. Tento režim neposkytuje rozdelenie výkonu.

### 2.5.6 Balance-tlb

Tento režim vyvažuje vysielaný prenos podľa peerov. Každá linka môže mať rozdielnu rýchlosť a duplex režim, nie je potrebná žiadna špeciálna konfigurácia prepínača ako pre iné režimy. Nevýhoda tohto režimu je, že podporuje iba MII pozorovanie linky a prichádzajúci prenos nie je vyrovnávaný. Primárny prenos bude používať linku, ktorá je nakonfigurovaná ako „základná“.

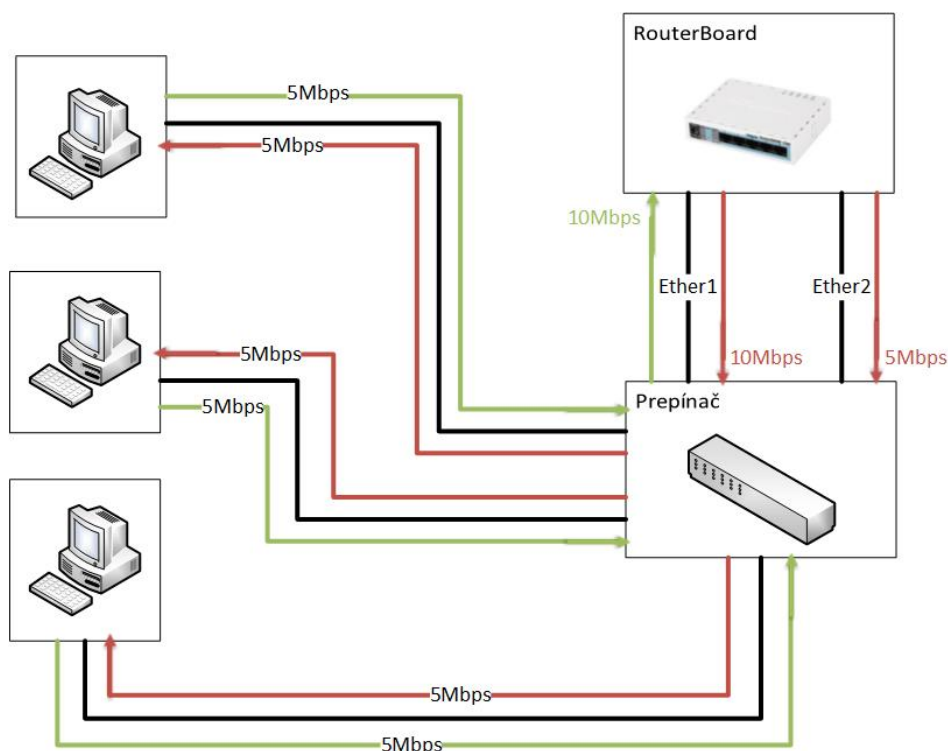
### 2.5.7 Príklad konfigurácie Balance-tlb

Prvá linka má najväčšiu šírku pásma tým pádom ju určíme za primárnu linku. Prepokladajme, že smerovač má dve linky ether1 maximálna šírka vlnového pásma je 10Mbps a ether2 má max 5Mbps. Prvá linka má väčšiu šírku, a teda tu nastavíme ako základnú linku.

```
/interface bonding add mode=balance-tlb slaves=ether1,ether2 primary=ether1
```

Pre prepínač nie je požadovaná žiadna ďalšia konfigurácia obr. 2.6 nám znázorňuje ako pracuje balance-tlb režim.

Ako môžeme vidieť smerovač dokáže komunikovať so všetkými klientmi pripojenými k prepínaču s celkovou šírkou vlnového pásma oboch liniek 15Mbps. Avšak ako už vieme, balance-tlb nevyrovnáva prichádzajúci prenos. V našom príklade dokáže



Obr. 2.6: Režim balance-tlb

klient komunikovať so smerovačom s úplnou šírkou základnej linky, ktorá má 10Mbps v našej konfigurácii.

### 2.5.8 Balance-alb

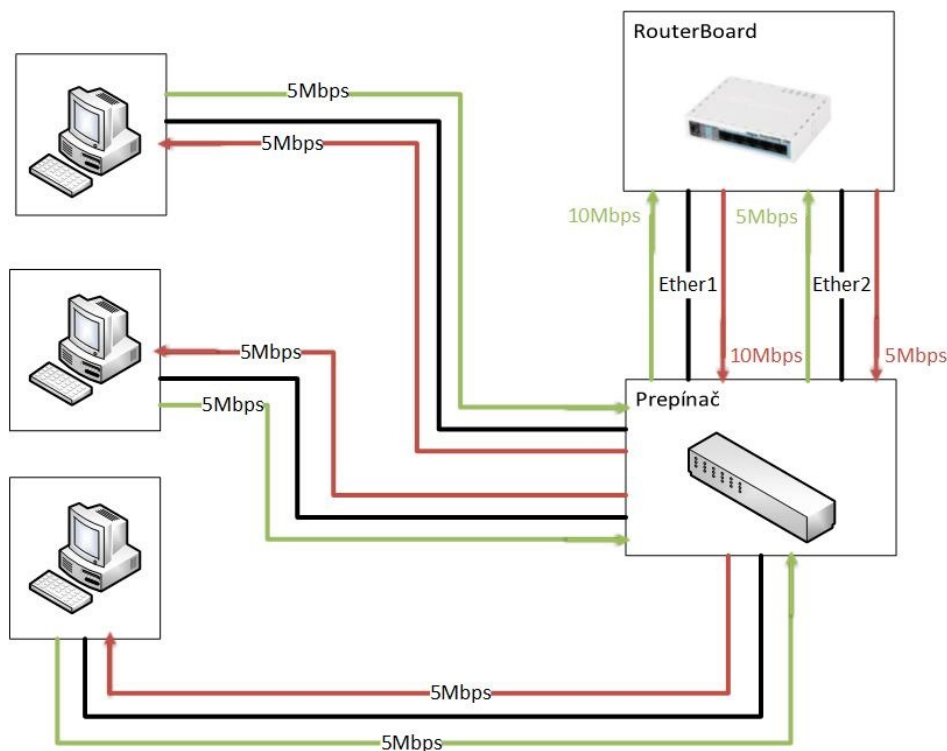
Tento režim je v podstate rovnaký ako balance-tlb, avšak aj prichádzajúci prenos je vyrovňovaný. Jediná nevýhoda je, že pre tento režim je potrebné zmeniť MAC adresu na konfigurácii ovládača, prístroja. Veľa lacných kariet nepodporuje tento režim obr. 2.7 znázorňuje činnosť balance-alb.

V porovnaní s balance-tlb režimom, na prenos od klienta môže byť taktiež použitá druhá linka na komunikáciu so smerovačom.

## 2.6 Address Resolution Protocol Monitoring

ARP Monitoring voľne preložené adresné rozlíšenie protokolu a jeho pozorovanie, posielajú vlastne ARP dotazy „Protokol rozlišovania adres pre rozhranie“ používa k tomu odpovede ako znamenia to znamená, že linka funguje. Tak isto nás uisťuje, že prebieha dátový prenos medzi linkami. Ak balance-rr a balance-xor režimy ktoré





Obr. 2.7: Činnosť balance-alb

sú popísané nižšie v texte, nastavené potom by mal byť prepínač nakonfigurovaný tak, aby rovnomerne distribuoval pakety po všetkých linkách. V opačnom prípade budú všetky odpovede z ARP cieľov prijaté na rovnakú linku, čo by mohlo spôsobiť zlyhanie ostatných liniek dokumentácia bola použitá z [2]

ARP pozorovanie je aktivované nastavením troch vlastností link-monitoringu, ďalej metóda na určenie monitorovania linky či je pripojená alebo odpojená. ARP-ip-targets vlastne IP cieľová adresa, ktorá bude pozorovaná ak link-monitoring je nastavený na ARP. Môžeme zadať viacnásobné IP adresy, ktoré oddelíme čiarkou a arp-interval, čas v milisekundách, ktorý definuje, ako často pozorujeme ARP požiadavky. Je možné špecifikovať hromadné ARP ciele, ktoré môžu byť užitočné v High Availability nastaveniach. Ak je nastavený iba jeden cieľ a to taký, že môže klesnúť. Tým, že máme viacej cieľov, sa zvyšuje spoľahlivosť ARP pozorovania.

Spustenie ARP pozorovania dosiahneme pomocou:

```
[admin@R1] interface bonding> set 0 link-monitoring=arp arp-ip-targets=172.16.0.2
[admin@R2] interface bonding> set 0 link-monitoring=arp arp-ip-targets=172.16.0.1
```

V našom príklade nezmeníme hodnotu arp-intervalu, RouterOS nastavuje arp-interval na 100ms automaticky. Odpojíme jeden z káblov, aby sme otestovali, či pozorovanie linky funguje správne, pozorujeme vypršanie času pingov, dokým arp monitorovanie nespozoruje chybu linky.

```
[admin@R1] interface bonding> /pi 172.16.0.2
172.16.0.2 ping timeout
172.16.0.2 64 byte ping: ttl=64 time=2 ms
172.16.0.2 ping timeout
172.16.0.2 64 byte ping: ttl=64 time=2 ms
172.16.0.2 64 byte ping: ttl=64 time=2 ms
172.16.0.2 64 byte ping: ttl=64 time=2 ms
```

## 2.7 Media independent interface Monitoring

Voľne preložené pozorované médiá nezávislé na rozhraní MII bola pôvodne definovaná ako štandardné rozhranie pre pripojenie Fast Ethernetu okolo 100 Mbit/s. MII Pozorovanie nám monitoruje iba stav miestneho rozhrania. V RouterOS je možné nakonfigurovať MII Pozorovanie dvomi spôsobmi.

- Prvým spôsobom je, že ovládač zariadenia určuje, či je linka pripojená alebo odpojená. Ak ovládač nepodporuje túto možnosť, bude sa linka vždy javiť ako pripojená.
- Druhým spôsobom je, že nižšie sekvencie volania vrátane jadra sú použité k určovaniu, či je linka pripojená. Táto metóda je menej efektívna, ale môže byť použitá pri všetkých zariadeniach. Táto metóda by mala byť použitá, iba ak nie je podporovaný MII prvý spôsob.

Hlavná nevýhoda je, že MII Pozorovania nám neurčuje, či môže linka skutočne prenášať pakety alebo nie, aj v prípade, že sa linka javí ako fungujúca. MII Pozorovanie sa nakonfiguruje nastavením rôznych link-monitoring režimov a mii-interval, ako často pozorovať linku, čo sa týka zlyhaní tento parameter sa používa iba v prípade, ak je link-monitoring v MII-1 alebo MII-2.

Ak chceme aktivovať MII druhý spôsob pozorovania musíme postupovať takto:

```
[admin@R1] interface bonding> set 0 link-monitoring=mii-2
[admin@R2] interface bonding> set 0 link-monitoring=mii-2
```

Takto mii-interval necháme na automatickej hodnote 100ms. Keď odpájame jeden z káblov, chyba bude v porovnaní s ARP pozorovaním rozpoznaná takmer okamžite.

## 2.8 Transmit hash policy

Určuje vlastne politiku vysielania hash, ktorá sa používa pri výbere slave a v režimoch balance-xor a 802.3ad dokumentácia bola použitá z [4]

- Layer-2 je požíva hlavne v XOR hardware a MAC adries na generovanie hash. Tento algoritmus umiestni všetku vašu návštevnosť na určitého sieťového partnera a na rovnakom podriadenom zariadení, tento algoritmus je samozrejme kompatibilný aj so štandardom 802.3ad.
- Layer-2 a Layer-3 toto pravidlo sa používa na kombináciu informácií druhej vrstvy a tretej vrstvy na generovanie hash. Používa sa taktiež XOR hardware MAC adries, IP adries na generovanie hash. Tento algoritmus umiestni všetku návštevnosť na určitého sieťového partnera na rovnakom podriadenom zariadení. Pre prevádzku bez IP je vzorec rovnaký ako pre politiku hašovania druhej vrstvy. Toto pravidlo má zabezpečiť vyváženejšiu distribúciu návštevnosti než samotná druhá vrstva a to najmä v prostredí, kde je potrebné zariadenie gateway tretej vrstvy a dosiahnuť najviac cieľov. Tento algoritmus je kompatibilný taktiež so štandardom 802.3ad.
- Layer-3 a Layer-4 táto politika používa informácie o protokole hornej vrstvy, ak sú k dispozícii na generovanie hash. To umožňuje návštevnosť určitého sieťového peeru na rozloženie viacerých podriadených, aj keď jediné spojenie sa nebude vzťahovať na viacerých podriadených. Pre fragmentované pakety TCP alebo UDP a pre všetky ostatné protokoly protokolu IP sa informácie o zdroji a cieľovom porte vynechajú. Pre prevádzku bez IP je vzorec rovnaký ako pre politiku hašovania druhej vrstvy. Tento algoritmus nie je plne kompatibilný so štandardom 802.3ad.

### 3 VÝSLEDKY MERANIA V LABORATÓRIU

V tretej kapitole sa venujeme získaným poznatkom a následne ich uplatňujeme pri konfigurácii a testovaní výkonnosti sieťových prvkov MikroTiku na začiatok sme testovali spojenie či nám daná konfigurácia bude fungovať. Neskôr sme si otestovali postupne všetky konfigurácie a postupne sme si uviedli príklady danej agregácie podľa štandardov IEEE802.3ad, balance-rr mnoho ďalších.

#### 3.1 Zapojenie

Na začiatok zo získaných poznatkov sme si pripravili schémy zapojenia kde sme v laboratóriu použili RouterBoard, prepínače a počítače. RouterBoardy boli použité 493C obr. 3.1

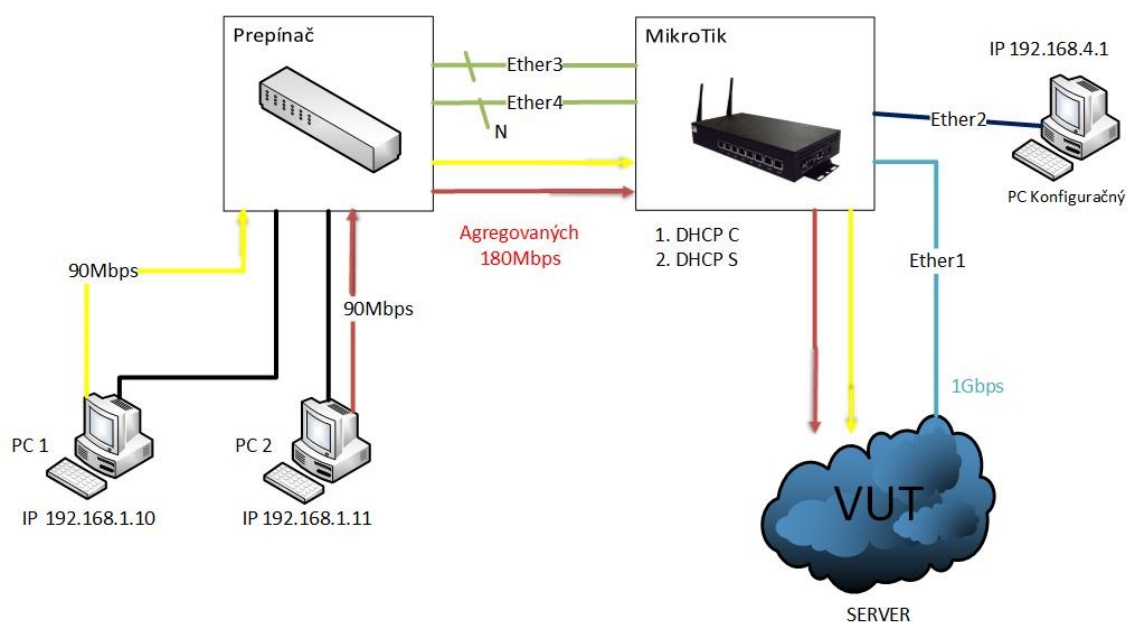


Obr. 3.1: RouterBoard 493C

#### 3.2 Meranie 802.3ad

Ako vidno podľa schémy zapojenia na obr. 3.2 bol v prvej konfigurácii použitý režim agregácie 802.3ad. Na MikroTiku boli nastavené DHCP server a DHCP klient tzn

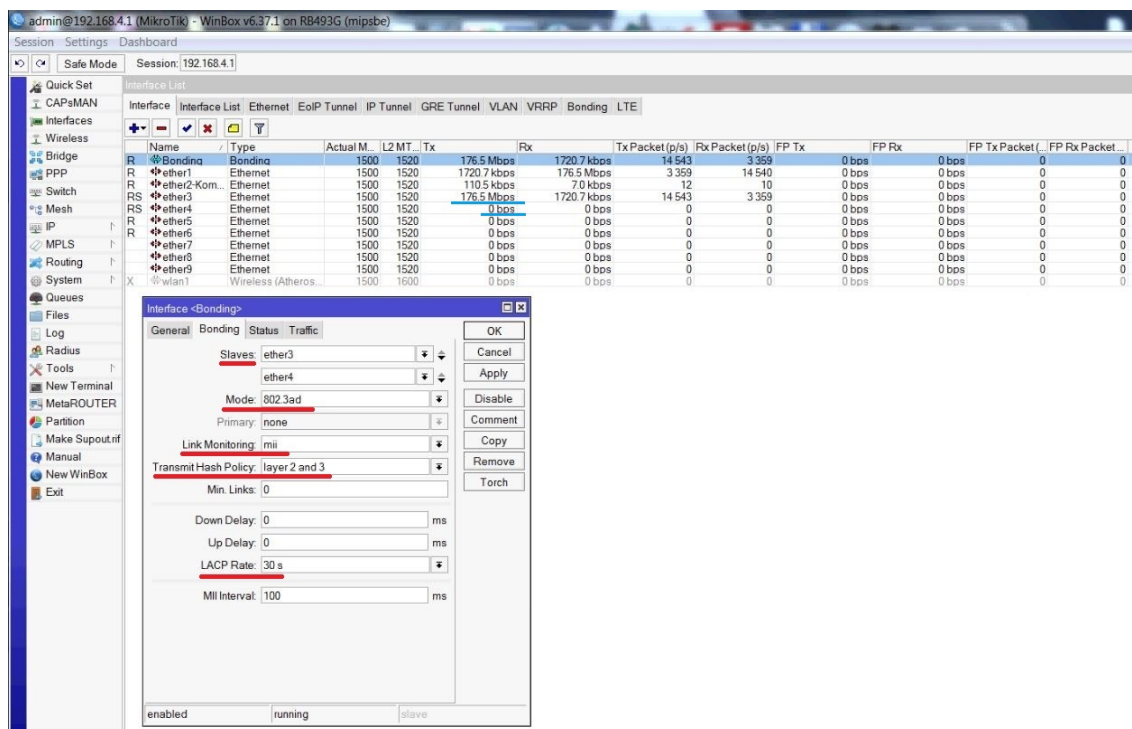
oba počítače mohli dostať IP adresu automaticky pri pripojení do MikroTiku respektíve prepínača. Konfigurácia smerovača bola použitá ako v kapitole 2.5.1 iba ethernet porty boli zmenené čiže interface bonding add slaves=ether3,ether4 mode=802.3ad lacp-rate=30secs link-monitoring=mii-type1 transmit-hash-policy=layer-2 a layer-3 a vidno ju aj na obr. 3.3 kde sú podčiarknuté červeným, už tu vidno prenos znázorňený modrou farbou, samozrejme pre prenos dát bolo nutné nastaviť aj prepínač.



Obr. 3.2: Schéma zapojenia 802.3ad

Prenos dát pri tomto režime konfigurácie bol po väčšinu času vyrovnaný tzn dosahoval od 150-180Mbps a dosahoval v priemere pri dvoch ethernetových lan kábloch 154,8Mbps obr. 3.4 to dokazuje kde sú hlavné parametre vyznačené červenou farbou. Obmedzenie medzi MikroTikom a prepínačom pri tomto režime nebolo použité, čo vyplývalo z teórie o tomto režime. Pri zmene konfigurácie, čiže pridaným ďalšieho ethernetového lan kábla nebola viditeľná žiadna zmena na vplyv prenosovej rýchlosti ani sa nezväčšila, ale ani nespomalila z toho usudzujeme, že dva ethernetové lan káble pre tento režim sú ideálne.

Dôležitým poznatkom bolo, že prenos dát prebiehal vždy cez jeden ethernetový port, čiže jedna fyzická cesta, ktorú má MikroTik v pamäti ako primárnu. Druhým dôležitým poznatkom bolo, že aj keď sme pridávali ethernetové lan káble tak žiadna zmena nenastala ani pri väčšom počte tzn 3,4,5 to nás len utvrdzuje v tom, že dva sú ideálne. Tento režim sa ukázal ako veľmi efektívny pri odolnosti voči chybám. Ďalšou

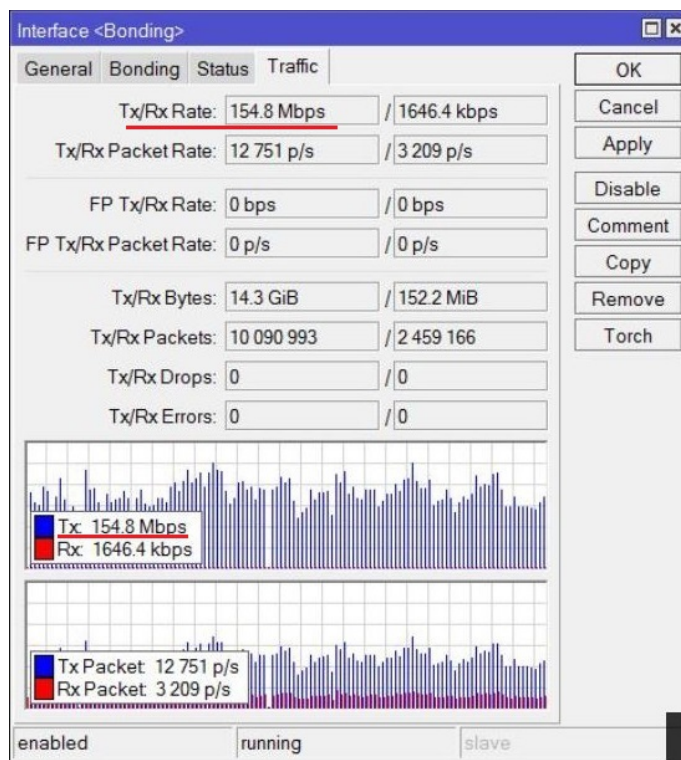


Obr. 3.3: Konfigurácia 802.3ad

možnosťou skúmania správania bolo použitie webového prehliadača, kde nám MikroTik ponúka možnosť vidieť jednotlivé grafy vyťaženia procesora, disku a pamäte ako na obr. 3.3 dôležité časti sú vyznačené na grafe. Tieto merania sú zobrazované v približne 5 minútovom intervale, čiže preto vidno len časť okolo 20 minút na každú z možností. Ako sa k týmto grafom dostať bolo už povedané v kapitole Winboxu. Keď MikroTik bežal pri tejto konfigurácii približne 30 minút začal byť dosť horúci tým pádom usudzujeme, že pri vyšších alebo väčších verziách MikroTiku je potrebná minimálne cirkulácia vzduchu alebo vstavaný ventilátor.

### 3.3 Meranie Balance–rr

Balance–rr ako voľne preložené rovnováha–rr bola zapojená obdobným spôsobom s jediným rozdielom bol pridaný tretí počítač. Keďže s teórie vyplýva, že tento režim bude prenášať pakety v striedavom poradí. Rozhodli sme sa že zapojíme tiež najprv dva ethernetové lan káble medzi MikroTikom a prepínačom a postupne budeme pridávať. Konfiguráciu opäť možno vidieť na obr. 3.6 kde sú vyznačené červenou farbou a prenos modrou, už na začiatku bolo vidieť že prenos bude rýchlejší ako pri režime 802.3ad.



Obr. 3.4: Prenos dát pri konfigurácii 802.3ad

Prenos dát pri tomto režime konfigurácie v priemere pri 10s a dvoch ethernetových lan kábloch 229,8Mbps. No keď sme pridali ďalší ethernet lan kábel prenos sa zvýšil na 284,7Mbps, pri štyroch ethernet lan kábloch to už bolo 307,2Mbps no to už bolo maximum, keďže piaty ethernet kábel už priniesol navýšenie na 307,4Mbps. Čiže môžeme povedať, že pri tomto režime je tri až štyri ideál. Záznam možno vidieť na obr. 3.7 kde boli použité najprv dva ethernetové lan káble a neskôr tri, jednotlivé prenosi sú vyznačené modrou farbou a spoločné červenou. Na druhom obr. 3.8 sú vidno naopak prenosi so štyrmi a piatimi eth. lan káblami tu tiež sú vyznačené modrým a spoločné červenou farbou. Balance-rr navyše nám zvyšuje výkon ale to za cenu nejakej tej fragmentácie čo by mohlo vytvárať problémy pri prevádzke s určitými protokolmi napríklad CIFS a to tiež s viacej ako dvoma sieťovými rozhraniami v našom prípade dvoma ethernetovými lan káblami. Z teórie ďalej vieme, že jeden paket nám spracuje jedna sieťová karta a ku ďalším treba naopak ďalšiu sieťovú kartu. Ak nám náhodou vypadne jeden ethernetový port tak sú nedoručené dáta naopak poslané cez ďalší avšak ak takýto existuje to je samozrejme podmienkou. Pri tomto režime užívateľ za použitia troch ethernetových lan kábloch dostaneme celkom slušnú užívateľskú prenosovú rýchlosť.

### 3.4 Meranie Active-backup

Ako už z názvu prezrádza tak sa bude jednať o režim aktívnej zálohy. Tu sme tiež použili schému z predošlých zapojení. Ako ďalej vyplýva, tak prenos bude prebiehať podobne ako pri 802.3ad len cez jeden aktívny ethernet port. No tu by mal užívateľ dostať náhradu spojenia pri výpadku jedného či viacej ethernet portov samozrejme podľa toho koľko je v sieti v zálohe. V tomto režime je možnosť určiť si primárny ethernet port vidno to aj na obr. 3.9 kde je znázornená konfigurácia červenou farbou.

Týmto portom bude prenos dáť pri normálnom režime prebiehať tu platí rovnako ako v predošlom že ak vypadne primárny port nahradí ho dočasne, alebo pri závažnej poruche na stálo iný. Na zázname ďalej vidno modrou farbou, že eth3, eth4 sú dočasne vyradené z prevádzky a na grafe že prenos sa obnovil skoro hneď. Prenosová rýchlosť pri tomto režime bola v dobe merania približne 157,2Mbps na obr. 3.9 je poznačená zelenou farbou. Čo je približne porovnateľné s 802.3ad.

### 3.5 Meranie Balance-tlb

Pri tomto režime bolo nutné iné zapojenie, ktoré vyplývalo z teórie ako v hore uvedených schému zapojenia vidno na obr. 3.10 tiež bolo v tomto režime nutné obmedziť linku medzi MikroTikom a prepínačom na 10Mbps download a 15Mbps upload na obr. 3.11 ho možno vidieť modrou farbou a konfiguráciu červenou, pretože jedine tak bolo vidno čo sa deje na príslušných portoch. Využité boli tri počítače na download, upload plus jeden konfiguračný, sledovací. Tento režim nám tiež zaručuje určitú odolnosť proti chybám a vyvažuje nám záťaž odchádzajúceho prenosu. Ak by náhodou jeden v našom prípade z ethernetových káblov bol nenávratne poškodený, alebo len čiastočne prevezme túto prevádzku ďalší a získa jeho MAC adresu.

Na obr. 3.11 ďalej možno vidieť zelenou farbou, že prenos bol rozdelený na obidva ethernetové porty ale s tým rozdielom, že download na eth3 bol 10,2Mbps, upload 10,3Mbps a na eth4 bol len download 6,0Mbps, upload žiadny čo aj vyplýva z teórie o tomto režime. Z tohto môžeme usudzovať ako funguje režim vyrovnávacieho vyrovnávania. Ako vidieť, MikroTik môže komunikovať so všetkými klientmi pripojenými k prepínaču s celkovou šírkou pásma oboch odkazov 16,2Mbps, ale ako už vieme, balance-tlb nevyvažuje prichádzajúcu prevádzku. V našom príklade môžu klienti komunikovať s MikroTikom a s celkovou šírkou pásma primárneho prepojenia čo je v našej konfigurácii 10,3Mbps. Ďalej sme skúšali pridávať jednotlivé ethernet lan káble medzi MikroTikom a prepínačom, ale nemalo to žiaden vplyv na prenos ako taký vždy sa len rozdelil download, ale upload ostal na eth3 stále rovnaký, čiže



na ostatných portoch bol upload vždy 0Mbps z čoho vyplýva, že upload bude vždy vedený cez jeden v našom prípade ethernetový port.

### 3.6 Meranie Balance–alb

Podobne ako v predchádzajúcom režime aj tu sme použili tri počítače a obmedzenie sme tu naopak nastavili na 15Mbps download, 15Mbps upload. Na schéme obr. 3.12 možno vidieť ako to môže byť rozdelené. Tento režim je veľmi podobný predchádzajúcemu a však s tým rozdielom, že tu nedochádza k vyvažovaniu predošlej prevádzky. Na obr. 3.13 vidíme nastavenú konfiguráciu červenou farbou a obmedzenie, ktoré vyššie spomíname modrou farbou.

Na obr. 3.13 je zelenou farbou naopak vidieť, že prenos prebiehal takto na eht3 bol download 4,4Mbps, upload 12,3Mbps a na ďalšom ethernetovom porte 10,3Mbps download a upload 3,8Mbps. Z toho nám vyplýva, že prenos sa rozdelil medzi obidva ethernetové porty a dokopy dával 15,4Mbps download, upload 15,4Mbps čo zasadný rozdiel oproti balance–tlb pretože tu prenos prebieha cez obidva ethernetové porty. V tomto režime sme opäť vyskúšali pridať väčší počet ethernetových pripojení medzi MikroTikom a prepínačom. No tu sa prenos vždy síce len rozdelil medzi ostatné ethernetové porty, ale výsledok ostal v podstate rovnaký a to, že približne sa blížil k hodnotám predchádzajúceho pokusu 15,4Mbps download, upload 15,4Mbps.

### 3.7 Meranie Broadcast

Tento režim nie až tak výnimočný, pretože u tohto režimu je prenos vedený na všetkých ethernetových portoch a nie je nijak obmedzovaný čiže dochádza k duplikáciám prenosu. Plus tento režim nám poskytuje iba odolnosť voči chybám. Prenos sa vždy len rozdelil medzi ethernetové porty v pomere 1:2 čiže pri dvoch ethernet kábloch bol na každom polovičný aj upload, download.

### 3.8 Meranie Balance–xor

Posledným režimom ktorý sme testovali bol práve balance–xor. Ako vyplýva z teórie vyššie tento režim má na výber z dvoch režimov transmit–hash–policy a to layer2–3, layer3–4. Test sme začínali s dvoma ethernetovými káblami ako predchádzajúcich pokusoch. Prenos bol vždy rozdelený medzi všetky aktívne porty pridávaním sa v podstate nič nezmenilo len sa dané rýchlosti podelili. Režim Balance–xor nám

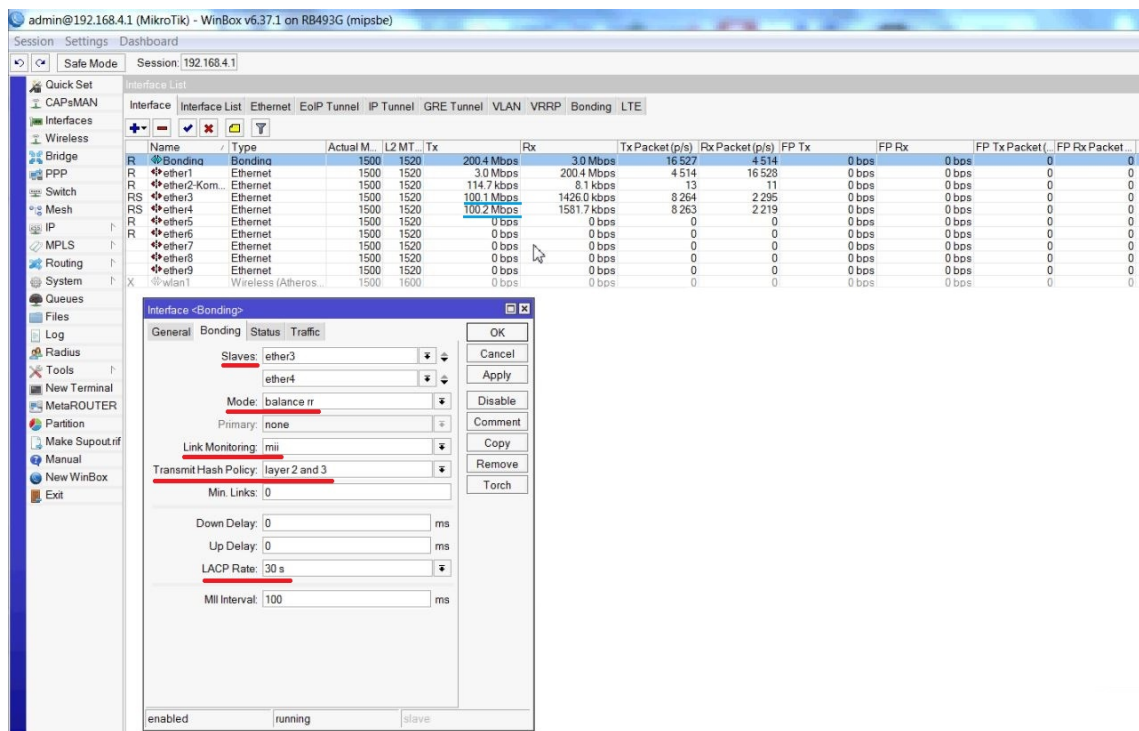
vyvažuje výstupné prenosy cez aktívne porty založené na hlavnom protokole s kontrolným súčtom informácii a prijíma prichádzajúce prenosy zo všetkých aktívnych portov. Režim je veľmi podobný s LACP okrem toho, že nie je normovaný a pracuje s vrstvou 3 a 4 hash politikou.

### 3.9 Porovnanie všetkých režimov

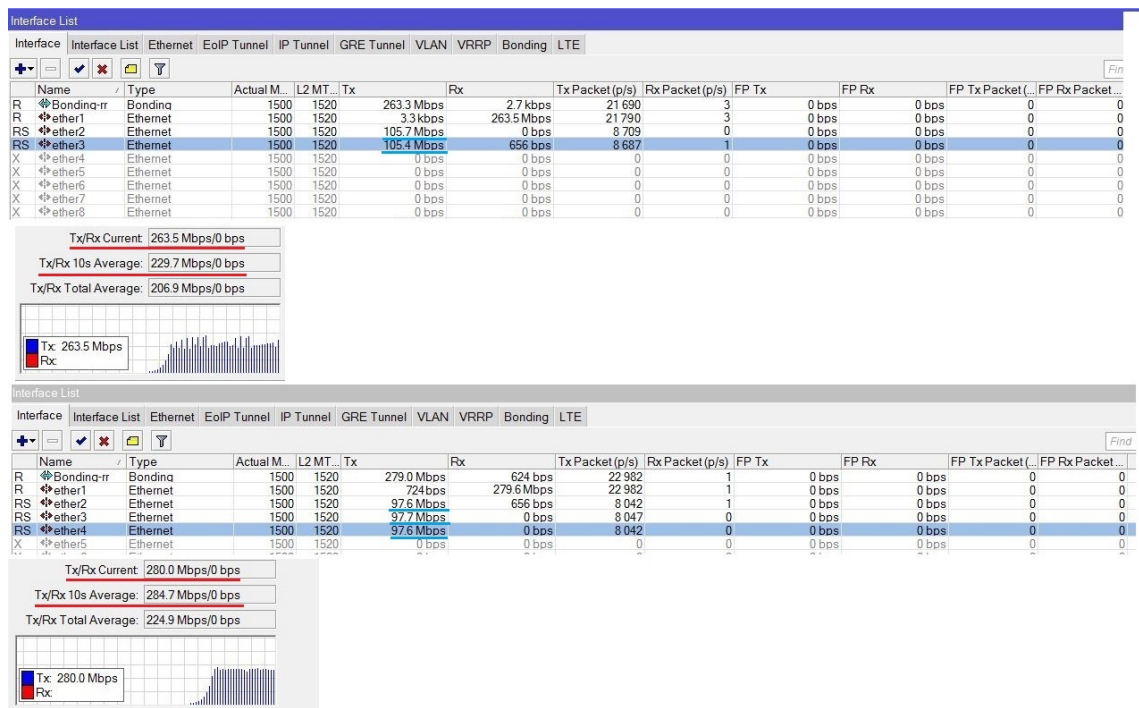
Ako vyskytlo z našich meraní, každý režim je niečím výnimočný a poskytuje nám iné vlastnosti. Všetky režimy od 802.3ad po balance-xor poskytujú odolnosť voči poruche no vyrovňovanie záťaže neposkytuje active-backup ani broadcast. Ostatné režimy vyrovňovanie záťaže poskytujú. Režim 802.3ad sa zdá ako najviac využívaný a pre svoju rýchlosť aj balance-rr kde sme dosiahli pri malom počte ethernetových káblov vyššiu prenosovú rýchlosť z tohoto hľadiska je určite pre bežného používateľa zaujímavý. Samozrejme ani aktívna-záloha nie je na zahodenie kedy by nejaká z liniek vypadla. Prechod z poškodenej linky bol takmer okamžitý z toho vyplýva, že tento režim je tiež zaujímavý. No ako bolo povedané tu bola prenosová rýchlosť o niečo menšia takže je len na užívateľovi aký režim si zvolí.



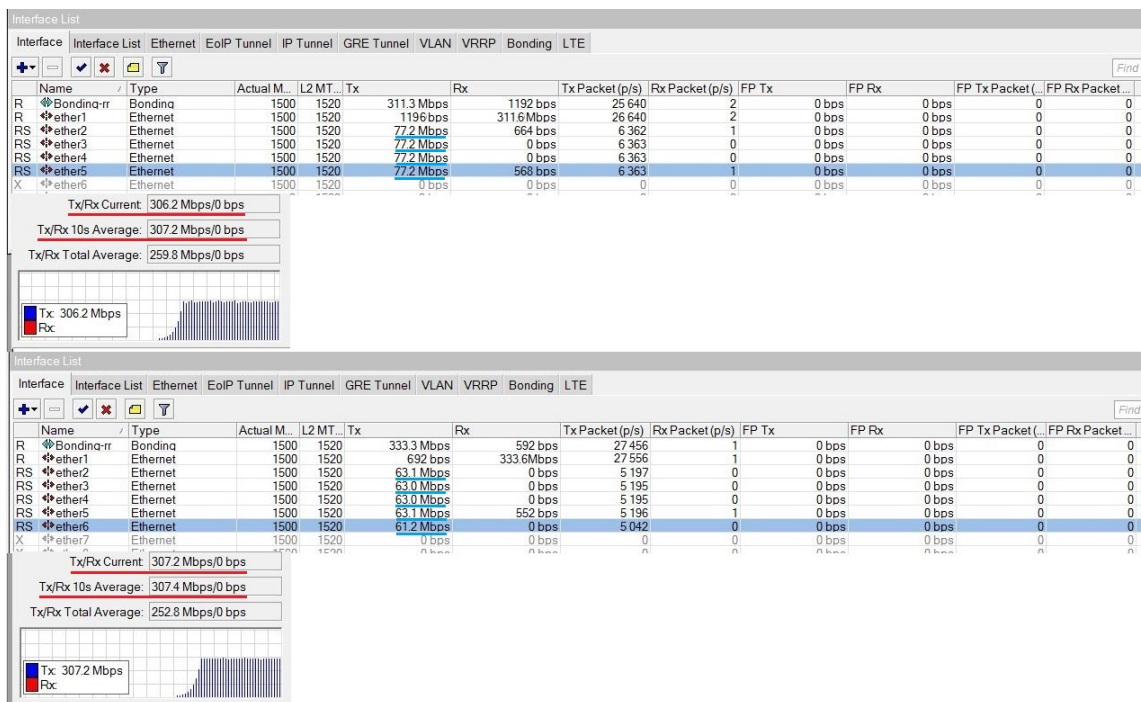
Obr. 3.5: Grafy vyťaženia pri konfigurácii 802.3ad



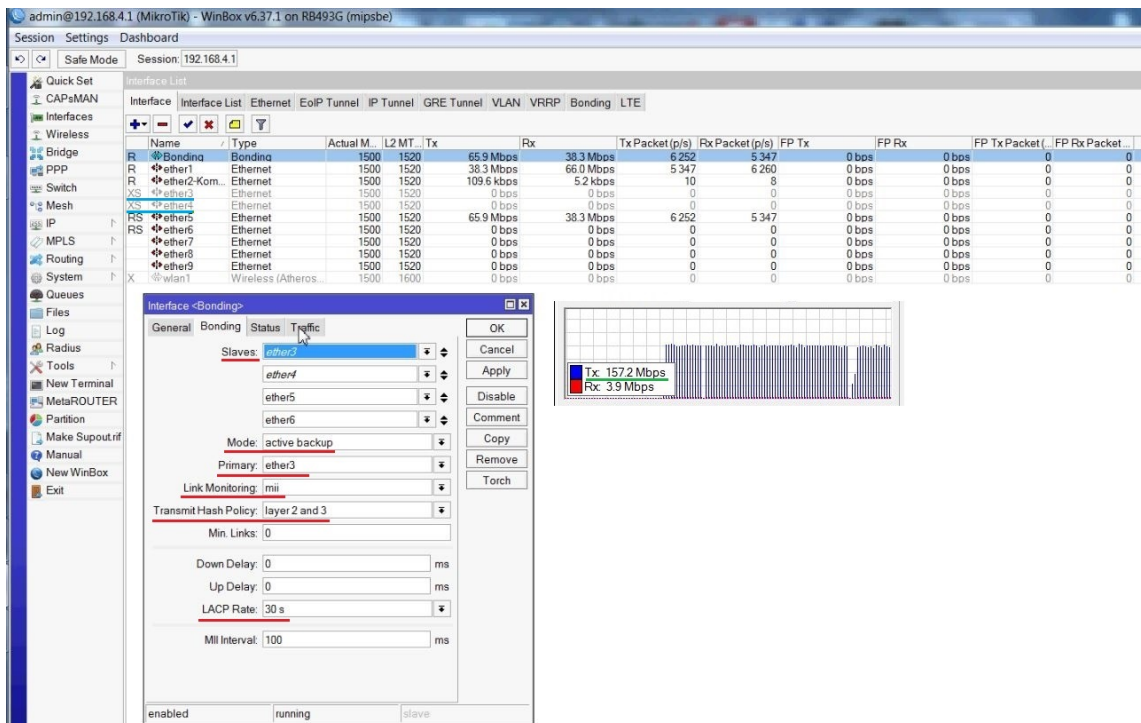
Obr. 3.6: Konfigurácia Balance-rr



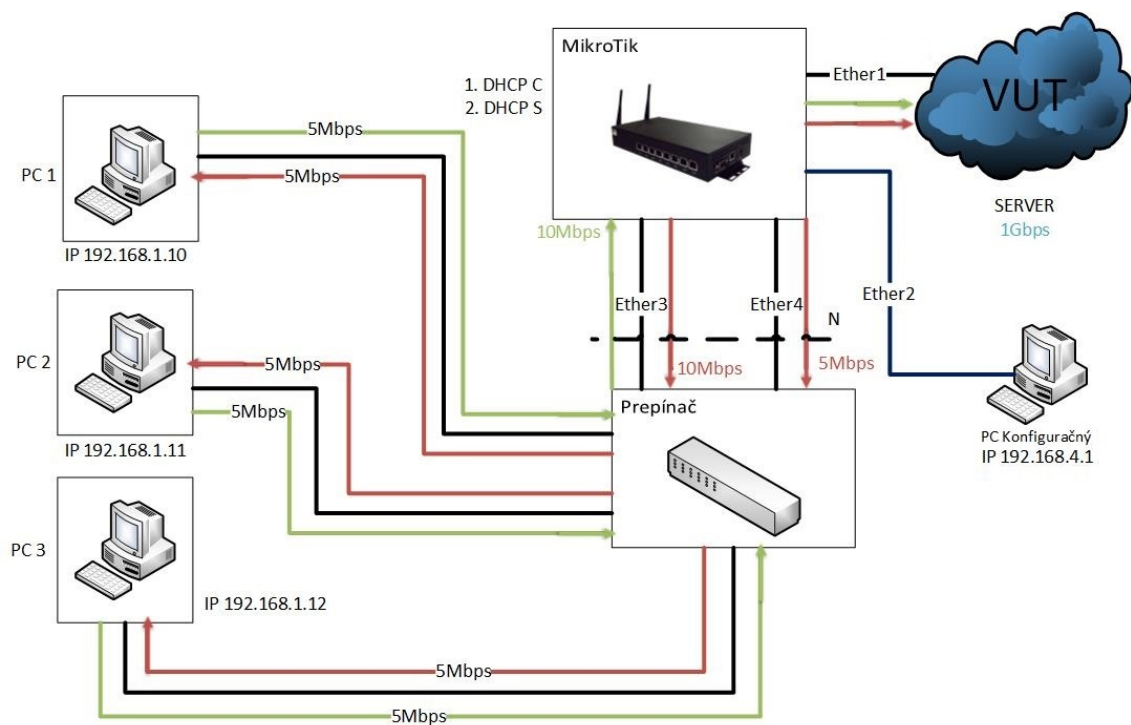
Obr. 3.7: Záznamy prenosu balance-rr pri dvoch a troch ethernet lan kábloch



Obr. 3.8: Záznamy prenosu balance-rr pri štyroch a piatich ethernet lan kábloch



Obr. 3.9: Záznam prenosu active-backup pri simulácii dvoch výpadkoch



Obr. 3.10: Schéma zapojenia balance-tlb

Session Settings Dashboard

Safe Mode Session: 6C3B6B424D A2

Interface List

Interface	Type	Actual M...	L2 MT...	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet...	FP Rx Packet...
R Bonding	Bonding	1500	1520	16.3 Mbps	10.5 Mbps	1823	1780	0 bps	0 bps	0	0
R ether1	Ethernet	1500	1520	6.9 Mbps	15.3 Mbps	1568	1448	0 bps	0 bps	0	0
R ether2	Ethernet	1500	1520	131.2 kbps	11.3 kbps	18	17	0 bps	0 bps	0	0
RS ether3	Ethernet	1500	1520	10.2 Mbps	10.3 Mbps	862	1523	0 bps	0 bps	0	0
RS ether4	Ethernet	1500	1520	6.0 Mbps	0 bps	790	0	0 bps	0 bps	0	0
R ether5	Ethernet	1500	1520	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ether6	Ethernet	1500	1520	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ether7	Ethernet	1500	1520	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ether8	Ethernet	1500	1520	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R ether9	Ethernet	1500	1520	0 bps	0 bps	0	0	0 bps	0 bps	0	0
X wlan1	Wireless (Atheros)	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0

Interface <Bonding>

General Bonding Status Traffic

Slaves: ether3 ether4

Mode: balance tlb

Primary: ether3

Link Monitoring: mii

Transmit Hash Policy: layer 2 and 3

Min Links: 0

Down Delay: 0 ms

Up Delay: 0 ms

LACP Rate: 30 s

MII Interval: 100 ms

enabled running slaves

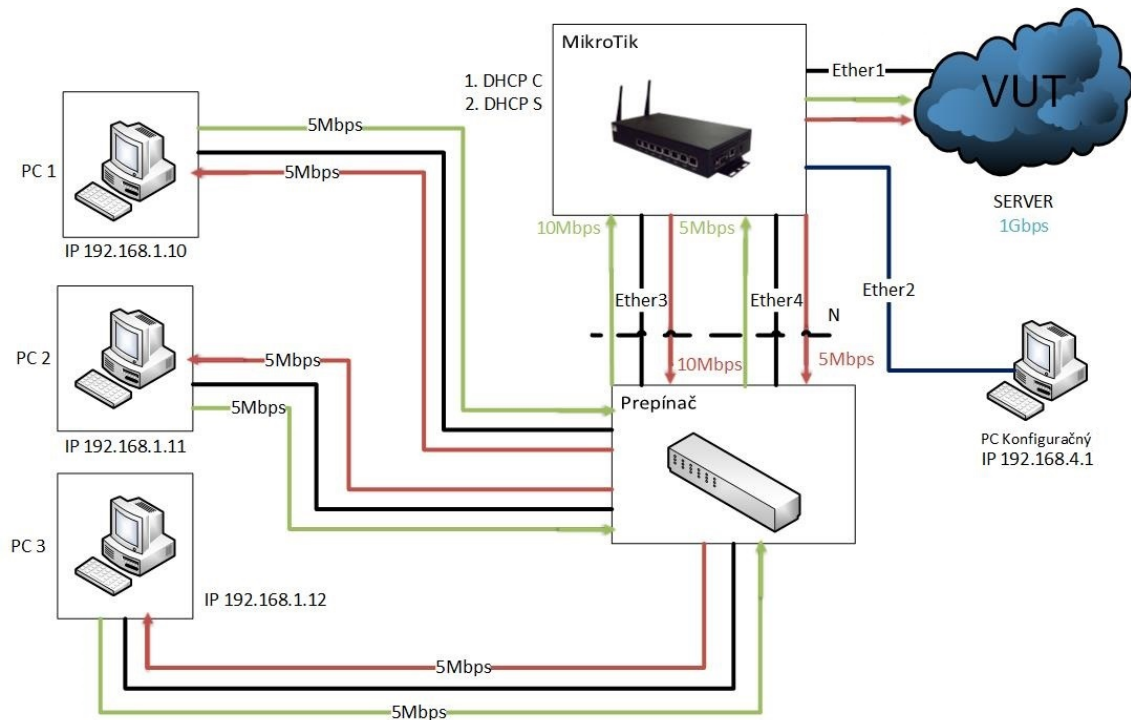
Queue List

#	Name	Target	Upload Max Li...	Download Ma...	Packet Marks	Total Max Limi...
0	Obmedzenie	Bonding	10M	15M		

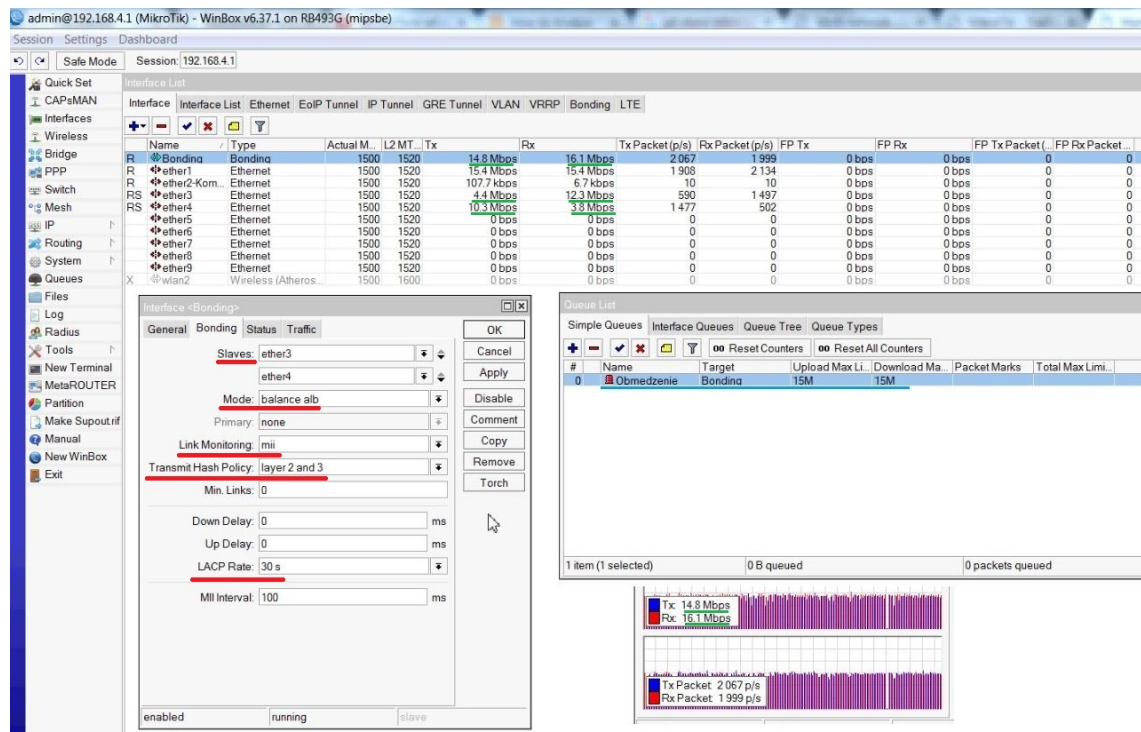
1 item (1 selected) 0 B queued 0 packets queued

Obr. 3.11: Prenos pri režime balance-tlb a znázornenie obmedzenia





Obr. 3.12: Schéma zapojenia balance-alb



Obr. 3.13: Prenos pri režime balance-alb a znázornenie obmedzenia

## 4 ZÁVĚR

V tejto bakalárskej práci sme si popísali Agregáciu Liniek na sieťovej vrstve MikroTiku, pomocou opisu protokolov a častí spájajúcich sa s ňou. Keďže história je vždy potrebná pre vysvetlenie a pochopenie danej problematiky bola vysvetlená na príkladoch jednotlivých protokolov. Keďže technologické zariadenia napríklad počítače či už to smerovače, alebo prepínače dnes komunikujú medzi sebou prostredníctvom protokolov, ktoré sú na to presne určené a na čo sa využívajú. Vzhľadom na to, že dnes už sú neoddeliteľnou súčasťou každej domácnosti či firiem práve počítače, notebooky alebo iné zariadenia od prepínačov a smerovačov tieto zariadenia využívajú protokoly, ktoré nám pomáhajú využívať tento virtuálny svet, v ktorom teraz žijeme a sú našou neoddeliteľnou súčasťou. Mnohí z nás si už ani nevieme predstaviť život bez týchto zariadení či už to život bez využívania komunikačných protokolov, ktoré nám uľahčujú komunikáciu a tým aj prácu pri prenášaní informácií, súborov a dát medzi inými počítačmi a zariadeniami.

V prvej základnej kapitole tejto bakalárskej práce sme sa venovali samotnej agregácii liniek kde sme si popísali jednotlivé protokoly ako aj ich históriu, vznik a ich základné vlastnosti.

V druhej kapitole sme sa venovali samotnému MikroTiku popisovali sme si kde táto spoločnosť sídli čomu sa venuje a čo vyrába. Venovali sme sa vlastnostiam RouterOS a ďalej sme sa venovali aj samotnému bondingu. Kde sme si na príkladoch vysvetlili aké môžu byť typy režimov, aké režimy môžeme použiť. Teóriu ich využitia a vlastnosti, ktoré majú.

V poslednej tretej kapitole sme mali možnosť získané poznatky uplatniť v praxi v laboratóriu, kde sme nadviazali spojenie medzi MikroTikom a inými zariadeniami. Samotná konfigurácia bola realizovaná pomocou winbox-u, ktorý bol opísaný v kapitole MikroTiku, že to nie je jediný spôsob úpravy konfigurácie bolo tiež vysvetlené v tejto kapitole. Niektoré grafy boli vytvorené pomocou tejto druhej možnosti, kde bola vidieť samotná vyťaženosť na MikroTiku. Samotný prenos bolo možné sledovať na MikroTiku a mohli sme sledovať aj niektoré grafy. Jednotlivé agregáčnne metódy boli tak porovnávané a ich slabšie a silnejšie stránky sa zobrazili v testoch jednotlivých režimoch. Naším výsledkom bolo porovnanie jednotlivých režimov využívajúcich pre účely agregácie sieťových liniek ako aj použitie pre samotného užívateľa. Ak by sme sa chceli lepšie pozrieť na budúcnosť, tak princípy agregácie sieťových liniek budú vždy určite aktuálne, pretože budú zaručovať určitý kompromis medzi investíciou a využívaním vyšších technológií, alebo existujúcich rezerv. Metódy vyrovnávania záťaže, obnovenie pri chybe, alebo výpadku spojenia, odstránenie chyby budú vždy na prvom mieste použitia.



# LITERATURA

- [1] Manual: Interface/Bonding *MikroTik documentation* [online]. 2016 [cit. 2016-01-13]. Dostupné z URL: <<http://wiki.mikrotik.com/wiki/Manual:Interface/Bonding>>.
- [2] Linux Foundation Wiki project *Bonding* [online]. 2017 [cit. 2017-02-09]. Dostupné z URL: <<https://wiki.linuxfoundation.org/networking/bonding>>.
- [3] Dallas, TX IEEE 802.3 *Maintenance IEEE 802.3* [online]. 2006 [cit. 2006-11-13]. Dostupné z URL: <[http://www.ieee802.org/3/maint/public/maint\\_open\\_1106.pdf](http://www.ieee802.org/3/maint/public/maint_open_1106.pdf)>.
- [4] UbuntuBonding *Descriptions of balancing algorithm modes* [online]. 2015 [cit. 2015-09-15]. Dostupné z URL: <<https://help.ubuntu.com/community/UbuntuBonding>>.
- [5] Link Aggregation Group Link Aggregation Control Protocol *An Intro: Protocols* [online]. 2016 [cit. 2012-05-22]. Dostupné z URL: <<http://www.excitingip.com/3015/>>.
- [6] Manual: Winbox *MikroTik documentation* [online]. 2016 [cit. 2016-09-19]. Dostupné z URL: <<http://wiki.mikrotik.com/wiki/Manual:Winbox>>.
- [7] About MikroTik *MikroTik: Company* [online]. Lotyšsko: Mikrotik, 2016 [cit. 2016-12-13]. Dostupné z URL: <<http://www.mikrotik.com/aboutus>>.
- [8] TechTarget *Definition for failover* [online]. 2016 [cit. 2005-09-01]. Dostupné z URL: <<http://searchstorage.techtarget.com/definition/failover>>.
- [9] Manual: Reset *MikroTik documentation* [online]. 2016 [cit. 2016-01-18]. Dostupné z URL: <<http://wiki.mikrotik.com/wiki/Manual:Reset>>.
- [10] Cisco *IEEE 802.3ad Link Bundling* [online]. 2016 [cit. 2006-10-04]. Dostupné z URL: <[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2sb/feature/guide/sbcelacp.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sbcelacp.html)>.
- [11] Manual: RouterOS FAQ *MikroTik documentation* [online]. 2016 [cit. 2011-09-11]. Dostupné z URL: <[http://wiki.mikrotik.com/wiki/Manual:RouterOS\\_FAQ](http://wiki.mikrotik.com/wiki/Manual:RouterOS_FAQ)>.
- [12] 802.3ad Ethernet Link Aggregation *802.3ad: Link Aggregation* [online]. 2016 [cit. 2012-06-26]. Dostupné z URL: <<https://www>>.

- juniper.net/techpubs/en\_US/junose13.2/topics/concept/802.3ad-link-aggregation-understanding.html>.
- [13] Corrigendum to IEEE Std 802.1AX *802.1AX: provides technical and editorial* [online]. 2016 [cit. 2016-01-01]. Dostupné z URL: <<http://ieeexplore.ieee.org/document/7600338/>>.
  - [14] 802.3ad Ethernet Link Aggregation *802.3ad: Link Aggregation: Public information* [online]. 2016 [cit. 2000-03-13]. Dostupné z URL: <<http://www.ieee802.org/3/ad/public/index.html>>.
  - [15] Link Aggregation: Extend Network *Link Aggregation to extend Network* [online]. 2016 [cit. 2011-01-20]. Dostupné z URL: <<http://www.excitingip.com/1103/why-not-use-link-aggregation-to-extend-your-network/>>.
  - [16] Advanced Networking *Link Aggregation and Failover: Configuration Examples* [online]. 2016 [cit. 2016-12-05]. Dostupné z URL: <<https://www.freebsd.org/doc/handbook/network-aggregation.html>>.

## SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ARP	adresné rozlíšenie protokol – Address Resolution Protocol
CIFS	bežný internetový súborový systém – Common Internet File system
DHCP	zoznam adres volných na použitie – Dynamic Host Configuration Protocol
DNS	systém doménových mien – Domain name system
FTP	protokol prenosu súborov – The File Transfer Protocol
IEEE	inštitút pre elektrotechnické a elektronické inžinierstvo – Institute of Electrical and Electronics Engineers
IP	komunikačný protokol – Internet Protocol
LACP	linkový agregáčny kontrolný protokol – Link Aggregation Control Protocol
LAG	linková agregácia v skupine – Link Aggregation Group
LAN	lokálna počítačová sieť – Local area network
MAC	riadenie prístupu k médiu – Media Access Control
MII	médiá nezávislé na rozhraní – Media independent interface
OSI	model sieťovej architektúry – Open Systems Interconnection
Ping	funkčnosť spojenia medzi dvoma sieťovými rozhraniami – Packet InterNet Groper
TCP/IP	primárny prenosový protokol/protokol sieťovej vrstvy – Transmission Control Protocol/Internet Protocol
UDP	používateľský datagramový protokol – User Datagram Protocol
VPN	virtuálna privátna sieť – Virtual Private Network
WAN	rozsiahla sieť – Wide Area Network